Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach

Rifaut, André; Feltus, Christophe

Published in:
In Proceedings of the CAISE 06 Workshop on Regulations Modelling and their Validation and Verification ReMo2V '06, Luxembourg

Publication date:
2006

Document Version
Early version, also known as pre-print

Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach

André Rifaut[1] and Christophe Feltus[1]

[1] Centre de Recherche Public Henri Tudor, 29, Avenue John F.Kennedy,
L-1855 Luxembourg-Kirchberg, Luxembourg
{Andre.Rifaut, Christophe.Feltus}@tudor.lu
http://www.tudor.lu

Abstract. The bankruptcy of financial institutions shows the rapid changes in the risks profiles of financial systems and processes. Although financial institutions have always managed the operational risks, the profile of this kind of risks is changing due to the increasing international competitive pressure and the evolution of the financial institutions' operational systems relying more and more on IT systems. This paper reports the results of the joint research with the CSSF [1] focusing on the formalization of both the Basel II Accord and compliant operational risk management (ORM) systems implementations. This formalization uses concepts of the ISO/IEC 15504 process assessment standard and the concepts of strategy and policy. This structure of the model ensures the traceability between the Basel II Accord and compliant ORM systems implementations, improves the formal validation of those systems and is more adequate to represent all organizational levels of financial institutions.

1 Introduction

In Luxemburg, the stability of the financial system is at the core of the economic stability of the country. The CSSF [1], which is the official authority for financial institutions supervision, has the responsibility to define financial regulations and ensure their fulfillment. This task is not easy because more and more international regulations are introduced, such as the IFRS [2], *Sarbanes-Oxley Act* (SoX) [2] and the Basel II Accord [3]. Audit managers, risk managers (including security managers), and compliance managers have developed standards addressing those regulations. For instance, Coso [2], CobIT [2], ITIL [18] and ERM [2] are governance and risk management standards. However, up to now there is nearly no integration between the regulations themselves and also between those standards. A joint research with the CSSF aims at defining a method for ensuring a correct implementation of financial systems compliant to Basel II regulation. The results [20,5] are based on quality methods and techniques, mainly goal-based models and analyses used in goal-oriented requirements engineering (GORE) [4]. The originality of the work lies in the formalization of the Basel II Accord and Operational Risk Management (ORM) systems by using concepts of the ISO/IEC 15504 process assessment standard [6] and the concepts of strategy and policy. This gives an adequate structure of the models at

all organizational levels of financial institutions, ensures the formal traceability between the Basel II Accord and ORM systems, and improves their formal validation.

This paper summarizes and extends the results of the joint research with the CSSF, focusing on the formalization of both Basel II Accord and compliant (ORM) systems implementations. More information on the research results, the ISO/IEC 15504 standard, the Basel II Accord, and other standards such as ITIL are freely available on the CSSF website [1]. The next section presents the main goals of this research and the preliminary results. Section 3 shows the technique that has been created in the context of the real case study concerning the Basel II Accord regulation and its implementation in financial institution. The last section summarizes the main results of this project and presents the future works that will be done within the follow-up research projects.

2 The Implementation of ORM Systems compliant to Basel II.

The Basel Committee has defined the operational risk as follows: it is *the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.* (§644 in [1]). As such, the operational risk encompasses all risks occurring at the operational and technical levels (see Fig. 1), in particular, all risks of the IT Software Engineering Processes (risks that concern project management, requirements analysis, design, security, ...). The methods used in IT Software Engineering (e.g. for safety and security analyses) do not cover the analysis of this very broad scope of risks.

The need for practical techniques is critical in order to help business units' manager to efficiently implement the core business processes that are under their responsibility. Indeed, not only the Basel II Accord is imposing constraints on those core financial processes, but also the other regulations (e.g. SoX, IFRS) are interfering on the same processes. Moreover, each regulation stresses the importance on a different but inter-related aspect. For instance, SoX stresses the importance on the reporting system also concerned by the ORM of Basel II Accord. In addition to that decisions about ORM system implementation must be made at the strategic, tactical, operational and technical levels. This increases the complexity of modeling and implementing ORM systems, taking into account also that operational risks exist in every business processes implying their strong relationships with new ORM systems. Last but not least, those regulations are hard to understand due to their lack of structure and lack of completeness. For instance, in the Basel II Accord there is no definition of important concepts such as "ORM system", "loss", "loss event", "expected loss", "unexpected loss", ...

Requirements engineering and goal-oriented methods. The GORE methods can overcome the difficulties presented in the preceding section by formalizing the Basel II Accord and the implementation of ORM systems. These methods can be used to analyze and model systems at all organizational level, from Business Models up to architectures [4]. Goal-oriented modeling languages are appropriate for that broad range of models and they support formal analyses. However, in the case of the ORM system, it is difficult to manage all of those large models and complex analyses.

Moreover, for validation purposes, it is important to refer to the concepts used in organizations, such as strategic objectives, strategies and plans, key indicators, policies, SLAs, ... Within the Basel II Accord context, additional structuring mechanisms has to be created on top of the usual goal-oriented concepts.

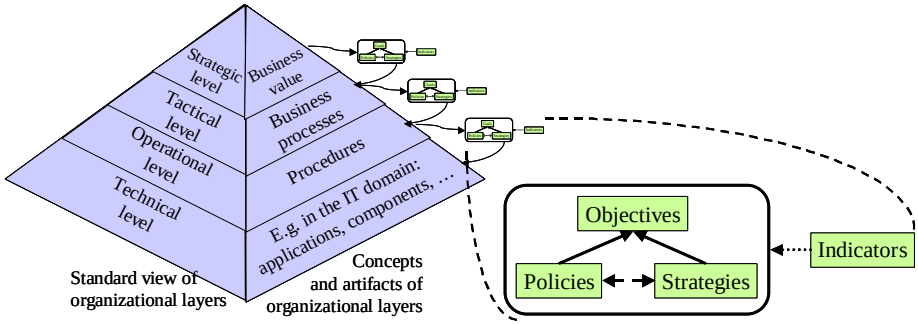

Fig. 1. The pyramid is used in management methods (e.g. [7]). The lowest 4 artifacts are defined with GORE models [4].

3 Formalizing Basel II and ORM with goal models and the ISO/IEC 15504 approach

The general framework given in the Figure 1, represented by the pyramid, is a standard view of the organization [7] used in financial institutions (and other institutions). The four organizational layers [8] – strategic, tactical, operational and technical levels – use concepts adapted to handle decisions at their corresponding abstraction level – that are mainly (respectively) business value [9], business processes, procedures and technical artifacts ([10]) such as IT applications in the IT domain.

ISO/IEC 15504 process assessment model. A first part of the structure is given by separating the description of the core activities of the business processes from the activities related to the capabilities of the business process (e.g. planning, work product control, process documentation, performance measurement, performance improvement, ...). As explained in [5], the benefits of this separation of concerns has proven to be very useful during the verification and the validation of the goal models. When describing process models with the ISO/IEC 15504 standard this separation of concerns is imposed. This new standard has been designed to be applicable for any business processes and is no longer limited to software engineering processes [20].

Objectives, strategies, policies and indicators. Those concepts (bottom of Figure 1) detail complementary aspects needed for designing business processes, procedures and technical artifacts. They are similar to organizational concepts needed in order to structure and formalize the links between each of the organizational levels [11].

When designing lower-level artifacts from higher level ones and when verifying the link between two organizational levels, one has to distinguish between the main objectives to be fulfilled, the strategy describing the approach to fulfill these objectives, the roles and responsibilities (policies) of the resources that will implement the strategies. Indicators are defined when there is a need for some monitoring, control, supervision or measurement concerning objectives, strategies or policies. Strategies and policies must be complementary and consistent with each other and they must fulfill the objectives.

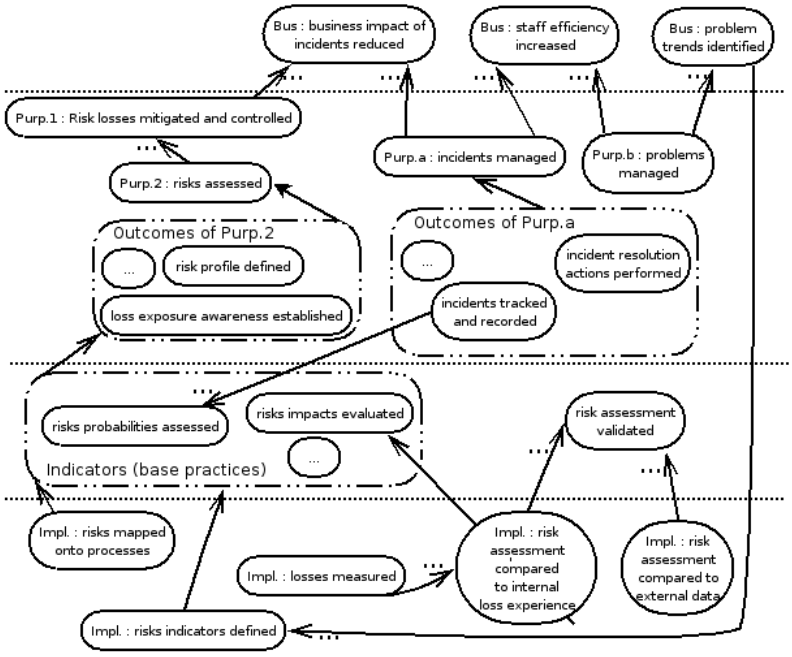

Fig. 2. Basel II ORM (left side) partially implemented (right side). Upside-down arrows shows that the implementation contributes to the each level of ORM.

The formal definition of those 4 concepts uses goal-oriented techniques [4,5]. For the indicators, our work is based on the Goal-Question-Metric method (GQM) [12]. Policies give a description of the roles and responsibilities (in accordance with [13] and policy management [14,15,16]) and allow detailing the authorizations, obligations (and their delegations), accountabilities, and separations of duties. Strategies give a description of the main approach or steps to fulfill given objectives. Our work follows [17] where strategies are integrated with goal-oriented analysis. For the sake of separation of concerns, responsibilities (and related aspects) are not defined in strategies but only in policies. Note that in financial institutions, the description of policies recalls its related objectives and strategies. This is also sometimes the case of strategies that gives a short description of their corresponding policies (i.e. description of roles and responsibilities). However, it is found essential to separate those descriptions when designing and analyzing those policies and strategies.

For instance, in the Figure 2, the diagram shows the model of the strategic level (topmost) and operational level (bottom). Only objectives are shown for those two levels. In between, at the tactical level, the objectives and indicators of business processes are shown. The left part of the diagram shows the Basel II Accord formalization of ORM. The right part presents a partial ORM system implementation using ITIL [18]. The links between the two models are formally analyzed [5].

4 Conclusions and Future Works

Building upon a method that has been defined within the setting of a real-case study in financial institutions, the Basel II Accord, new results are presented in this paper aiming at giving a simple but integrated set of concepts – goals, indicators, policies and strategies – which can be used to design financial systems compliant to regulations and structure their analysis in relationship with the artifacts commonly used in financial institutions – business models, business processes models, procedures and more technical artifacts. The formalization of goals, indicators, policies and strategies independently from each other allows analyzing and recording the design decisions across all organizational levels, making easier the link with the regulation. The main advantage of this method is that it keeps the structuring power of the ISO/IEC 15504 capability model that can be used to discover weaknesses and operational risks in the business process implementation with the method explained in [19]. Based on the same techniques as in [15], a prototype implementation is under development.

The current and future works of the authors focus on a constructive method aiming at giving an effective support for financial business process design (compliant to regulations), establishment, assessment, improvement, governance and benchmarking [5]. In particular, a risk and value analysis method is under development adapted to process assessment, improvement and governance. Some support is also given to another research made by experts in DPM [21]. The aim of those experts is to ground digital policy management in sound non-federated distributed IT systems that enforces policies fulfillment even outside the traditional IS frontier of each institution. Finally, the current project with the CSSF is still in progress with results that are extended to the IFRS [2] concerning the management of unquoted assets (IFRS-IAS39) [2]. In addition to model this regulation and the systems compliant to it, the relationship between IFRS-IAS 39 and Basel II can be analyzed and alternative compliant implementations of integrated systems can also be designed.

References

1. CSSF: Commission de Surveillance du Secteur Financier. The firsts results of the joint project are freely downloadable at http://www.cssf.lu/index.php?id=130 .
2. IFRS: International Financial Reporting Standards, IASCF, USA. SoX: Sarbanes Oxley Act of 2002, USA. COSO: Internal Control – Integrated Framework, CSOTC, USA. CobiT®: Control Objectives for Information and related Technology, ISACA, USA. ERM: Enterprise Risk Management – Integrated Framework, CSOTC, USA.
3. Basel Committee on Banking Supervision, “International Convergence of Capital Measurement and Capital Standards”; BIS; Basel, June 2004.
4. A. van Lamsweerde, "Goal-Oriented Requirements Engineering: A Guided Tour". Invited minitutorial, Proc. RE'01 - International Joint Conference on Requirements Engineering, Toronto, IEEE, August 2001, pp.249-263.
5. André Rifaut, “Goal-Driven Requirements Engineering for Supporting the ISO 15504 Assessment Process”, EuroSPI 2005, Budapest
6. ISO/IEC 15504, “Information Technology – Process assessment”, (parts 1-5), 2003-2006 (see website [1] for details about this standard).

7. Anthony, R. N. Planning and Control Systems: A Framework for Analysis. Harward University, Boston, USA, 1965
8. Henderson, J. and Venkatraman, N., “Strategic alignment: Leveraging technology for transforming organizations”. IBM Systems Journal, 1999, 38.
9. Osterwalder and Pigneur. An Ontology for e-business models. In “Value Creation from E-Business Models”, Wendy Currie ed., Butterworth-Heinenmann. Apr 2005.
10. Robson W, Strategic Management and Information Systems, Pitman, 1997.
11. Chaffey et al. (2005) - Business Information Systems: Technology, Development and Management for the E-business, Prentice Hall.
12. Van Solingen, “The Goal/Question/Metric Method: A Practical Guide For Quality Improvement of Software Development”, McGraw-Hill, Jan. 1999
13. René Wies, “Using a Classification of Management Policies for Policy Specification and Policy Transformation”. In Proc. ISINM '95, Santa Barbara, California, May 1995.
14. N. Damianou, N. Dulay, E. Lupu, and M. Sloman, “The ponder policy specification language” In Morris Sloman, (ed), Proc. of Policy Worshop, 2001, Bristol UK, January 2001.
15. A. Schaad and J. Moffett. “Delegation of obligations.” In IEEE Policy Workshop, 2002
16. Qingfeng He and Annie I. Antón, “Deriving Access Control Policies from Requirements Specifications and Database Designs”, ICSE 2005.
17. Rolland C., N. Prakash, A. Benjamen, “A multi-model view of process modelling.” Requirements Engineering Journal, p. 169-187,1999.
18. ITIL: IT Infrastructure Library – Service Support, Service Delivery, published by OGC, London. (see website [1] for details about this standard).
19. A. Rifaut, M. Picard and B. Di Renzo, “ISO/IEC 15504 Process Improvement to Support Basel II Compliance of Operational Risk Management in Financial Institutions”,International Conference SPiCE 2006.
20. B. Di Renzo, M. Hillairet, M. Picard, A. Rifaut, C. Bernard, D. Hagen, P. Maar, D. Reinard, “Operational Risk management in Financial Institutions: Process Assessment in Concordance with Basel II”, International Conference SPiCE 2005.
21. J.-H. Morin and M. Pawlak, “Towards a Global Framework for Corporate and Enterprise Digital Policy Management”, SoftWars conference, Las Vegas, USA, Dec 11, 2005.